Unconditional security of key distribution from causality constraints

Lluís Masanes
ICFO-Institut de Ciencies Fotoniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain

Renato Renner
Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland

Matthias Christandl
Arnold Sommerfeld Center for Theoretical Physics, Faculty of Physics, Ludwig-Maximilians-University Munich, 80333 Munich, Germany

Andreas Winter
Department of Mathematics, University of Bristol, University walk, Bristol BS8 1TW, U.K.
Centre for Quantum Technologies, National University of Singapore, 2 Science Drive 3, Singapore 117542

Jonathan Barrett
H. H. Wills Physics Laboratory, Tyndall Avenue, Bristol BS8 1TL, U.K.

(Dated: December 10, 2009)

We analyze a protocol which generates secret key from correlations that violate a Bell inequality by a sufficient amount, and prove its security against eavesdroppers which are only constrained by the fact that any information accessible to them must be compatible with the impossibility of arbitrarily fast signaling. We prove unconditional security according to the strongest notion, the so called universally-composable security. The no-signaling assumption is imposed at the level of the outcome probabilities given the choice of the observable, therefore, the protocol remains secure in situations where the honest parties do not have a complete control over their quantum apparatuses, or distrust them. The techniques developed are very general and can be applied to other Bell inequality-based protocols. In particular, we provide a scheme for estimating Bell-inequality violations when the samples are not independent and identically distributed.

I. INTRODUCTION

In entanglement-based protocols for quantum key distribution (QKD) [1] two honest parties (Alice and Bob) can obtain a secure secret key by performing measurements on shared EPR pairs [2]. They can also certify that they have EPR pairs by observing sufficiently strong violations of Bell inequalities [3–5]. When the EPR pairs are noisy, measurements lead to noisy and partially secret correlations. In order to obtain perfect secret bits, error correction and privacy amplification have to be performed, with the assistance of local operations and public communication (LOPC) [6]. Before implementing this procedure, however, an estimate of the quality of the correlations needs to be performed. Formulated in a different way, an estimate of the maximal amount of information that an eavesdropper (Eve) has about Alice's and Bob's bits has to be performed. This is done by exploiting the monogamy of entanglement, which imposes trade-offs between the entanglement between Alice and Bob, and Eve's correlations with them [7].

A way of estimating the degree of entanglement that Alice and Bob share is to perform quantum tomography [8]. In order to do so, they have to assume that the quantum systems they measure live on a state space of a particular dimension d (usually two). This assumption, though strong, is usually not mentioned in the presentations of QKD. In particular, it implies that Alice and Bob must trust their apparatuses (see [9] for a detailed discussion).

A framework in which one can analyze quantum correlations without knowledge of the dimension d is to consider them in the larger set of no-signaling correlations [10]. No-signaling correlations are characterized by the assumption that *no measuring process can be used to send information between distant locations*. In this framework, the origin of the correlations, the kind of system that has been measured, and in particular, the dimension d of the underlying quantum system, do not matter. It is shown in [10] that, if the obtained correlations violate some Bell inequality then there is some degree of privacy in them—in the sense that secret key is needed to create these correlations by LOPC.

The first protocol proved secure against a no-signaling eavesdropper is the BHK-protocol, introduced in [11]. However, the security analysis provided was limited, it only applies to the noiseless regime and has a vanishing secret key rate. In [12] it was shown that the BHK-protocol with a positive key rate is secure against individual attacks, even in the noisy regime. In the present paper we generalize this result to completely general attacks. The security definition that we use is the strongest

one, the so called *universally-composable security*. One calls a cryptographic primitive (for instance key distribution) universally composable if it is secure in any arbitrary context (for instance one-time pad encryption) [13, 14]. The secret key rate that we obtain is comparable to the one obtained when the eavesdropper is constrained by quantum mechanics, and when the devices are fully specified and trusted.

In order to do so, we introduce an exponentially-accurate scheme for estimating symmetric properties of arbitrary multipartite probability distributions. Also, we prove the security of privacy amplification in a similar way as in [15]. Our proof has the advantage that can accommodate any error-correction scheme.

The paper is structured in the following way. In Section II we introduce some preliminaries: nonsignaling correlations, nonlocality, and their relation to privacy. In Section III we describe the protocol, and explain how to implement it with quantum devices. In Section IV we explain the security criterion. In Section V we compute the secret key rate in a practical scenario. In Section VI we provide the complete security proof, distributed in several subsections. Section VII contains the conclusions.

II. PRELIMINARIES

A. Nonsignaling correlations

We use upper-case A to denote the random variable whose particular outcome is the corresponding lower-case a. We use bold letters to denote strings of variables $\mathbf{a} = (a_1, \ldots, a_N)$ or random variables $\mathbf{A} = (A_1, \ldots, A_N)$.

Alice and Bob share N pairs of physical systems, labeled by $n \in \{1, \ldots, N\}$. Alice measures her n^{th} system with one of the M observables $X_n \in \{0, 1, \ldots, M-1\}$, obtaining the outcome $A_n \in \{0, 1\}$. Analogously, Bob measures his n^{th} system with one of the $(M+1)$ observables $Y_n \in \{0, 1, \ldots, M\}$ and obtains the outcome $B_n \in \{0, 1\}$. The chosen observables and their corresponding outcomes for the N pairs of systems are represented by the random variables $\mathbf{A}$, $\mathbf{B}$, $\mathbf{X}$, $\mathbf{Y}$, which are correlated according to the joint conditional probability distribution $P_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y}}$. The number $P_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y}}(\mathbf{a}, \mathbf{b}, \mathbf{x}, \mathbf{y})$ is the probability of obtaining the strings of outcomes $\mathbf{a}, \mathbf{b} \in \{0, 1\}^N$ when measuring $\mathbf{x} \in \{0, \ldots, M-1\}^N$ and $\mathbf{y} \in \{0, \ldots, M\}^N$. The only assumption about this distribution is the following.

The no-signaling assumption: *The choice of observable for one system cannot modify the marginal distribution for the rest of systems.*

More formally, we impose the following condition among any two sets of subsystems with input I_1, I_2 and output O_1, O_2:

$$\sum_{o_2} P_{O_1,O_2|I_1,I_2}(o_1, o_2, i_1, i_2) = \sum_{o_2} P_{O_1,O_2|I_1,I_2}(o_1, o_2, i_1, i_2')$$

for all i_2, i_2', o_1, i_1. Although the two sets of subsystems are arbitrary, the above constrains turn out to be equivalent to the ones where (O_2, I_2) corresponds to a single subsystem (A_n, X_n) or (B_n, Y_n). It is important to note that if these equalities were not satisfied, arbitrarily fast signaling between separated subsystems could be achieved. Also, if not for this assumption, the notion of subsystem would have no sense. General properties for nonsignaling correlations are shown in [10].

In the cryptographic scenario one assumes that the only information accessible to Eve (apart from the public messages exchanged by Alice and Bob) is the outcome E obtained when measuring a physical system with an observable Z. Without loss of generality we assume that Eve has only one system. The sole assumption that we use in the security proof is that the global $(2N+1)$-partite distribution $P_{\mathbf{A},\mathbf{B},E|\mathbf{X},\mathbf{Y},Z}$ is a nonsignaling one. Apart from this, this distribution is completely arbitrary.

It is important to stress that systems inside Alice's laboratory must not signal each other, and the same for Bob. This may be quite difficult to implement in practice, but it is, in principle, possible.

B. Nonlocality and privacy

A bipartite distribution $P_{A,B|X,Y}$ is said to be local if it can be written as

$$P^{\text{local}}_{A,B|X,Y} = \sum_v P_V(v)\, P_{A|X,V}(v)\, P_{B|Y,V}(v)\ . \qquad (1)$$

Local distributions can be generated by shared randomness (denoted V above) between the parties, plus local operations. A distribution $P_{A,B|X,Y}$ which cannot be written as (1) is said to be nonlocal.

By definition, Bell inequalities [3–5] are satisfied by all local distributions (1). In this paper, we concentrate on the Braunstein-Caves (BC) Bell inequality [5]. For any distribution $P_{A,B|X,Y}$ with $A, B \in \{0, 1\}$ and $X, Y \in \{0, \ldots, M-1\}$, let $P_{X,Y}$ be uniform on the set

$$\{(x, y) : y = x \text{ or } y = x + 1 \bmod M\}\ , \qquad (2)$$

and define the random variable

$$\mathcal{B}[A, B, X, Y] = \frac{1}{2} + M\big(A \oplus B \oplus \mathrm{I}\{X = M-1\}\mathrm{I}\{Y = 0\}\big) \qquad (3)$$

where the indicator function is defined as $I\{\text{true}\} = 1$, $I\{\text{false}\} = 0$. The BC-inequality for M observables [5] can be written as

$$\langle \mathcal{B} \rangle \geq 1\ . \qquad (4)$$

The bipartite distribution $P_{X,Y}$ can be generated between two noncommunicating parties in the following way: (i) X, Y are independently generated with uniform distribution over $\{0, \ldots, M-1\}$, (ii) after the measurements, once communication is allowed, the two parties post-select the evens where (X, Y) is in the set (2). As mentioned above, any local distribution (1) satisfies (4). The BC-inequality for $M = 2$ is equivalent to the CHSH-inequality [4]

$$\left\langle A \oplus B \oplus \mathrm{I}\{X = 1\}\mathrm{I}\{Y = 0\} \right\rangle \geq \frac{1}{4} \ , \tag{5}$$

where here, the random variables X, Y are independent and uniform on $\{0, 1\}$.

Suppose that Eve is correlated to Alice through the global distribution $P_{A,B,E|X,Y,Z}$. If Alice measures $X = 0$, we can quantify the knowledge that Eve has about A with the (optimal) correct-guessing probability

$$\mathcal{P}_{\mathrm{guess}}(A|E) = \max_z \sum_e \max_a P_{A,E|X,Z}(a, e, 0, z) \ . \tag{6}$$

If $\mathcal{P}_{\mathrm{guess}}(A|E) = 1$ then Eve knows A with certainty. If $\mathcal{P}_{\mathrm{guess}}(A|E) = 1/2$ then Eve is completely ignorant about the value of A. In this paper it is shown that the knowledge that Eve has about A can be upper-bounded by the amount of nonlocality that Alice and Bob share

$$\mathcal{P}_{\mathrm{guess}}(A|E) \leq \langle \mathcal{B} \rangle \ . \tag{7}$$

If the marginal for the honest parties $P_{A,B|X,Y}$ violates the BC-inequality (4), then according to (7), the probability that Eve guesses correctly is smaller than one. This is the reason why the Bell inequality (4) is unconventionally written as a lower bound: the more nonlocality the honest parties share, the lower $\langle \mathcal{B} \rangle$ is, and the less knowledge Eve has (7). This is one manifestation of the monogamy of nonlocal correlations [10].

III. THE PROTOCOL

A. Implementation with quantum devices

Here we explain how to implement the protocol with quantum-mechanical devices. This is not necessary for defining the protocol, or prove its security. However it helps to understand the reasons behind its particular design.

Suppose Alice and Bob share many copies of the noisy EPR state

$$\rho = p\,\Phi + (1-p)\frac{\mathbb{I}}{4} \ , \tag{8}$$

where $0 \leq p \leq 1$ is the purity, Φ is the projector onto $|00\rangle + |11\rangle$, and $\mathbb{I}$ the four-dimensional identity matrix.

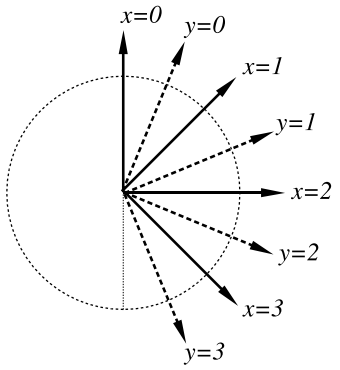

FIG. 1: Location in the equator of the Bloch sphere of the observables for $M = 4$.

They perform the measurements in the following orthogonal basis. The observable $x \in \{0, \ldots, M-1\}$ for Alice is

$$|0\rangle \mp e^{i\pi \frac{x}{M}} |1\rangle \ , \tag{9}$$

the observable $y \in \{0, \ldots, M-1\}$ for Bob is

$$|0\rangle \mp e^{-i\pi \frac{y+\frac{1}{2}}{M}} |1\rangle \ , \tag{10}$$

and the observable $y = M$ for Bob is

$$|0\rangle \mp |1\rangle \ , \tag{11}$$

the same as Alice's $x = 0$. In the Bloch sphere, these observables correspond to the directions represented in FIG. 1. The observables $x, y \in \{0, \ldots, M-1\}$ are the ones used to obtain large violations of the BC-inequality [5]. For $M = 2$, the settings (9, 10) are the ones which maximize the violation of the CHSH-inequality [4] for the state (8). The observables $x = 0, y = M$ maximize the correlation between Alice and Bob, and hence, are used to generate the raw key.

B. Description of the protocol

Recall that for each value of M we have a different protocol.

1. Distribution and measurements. Alice and Bob are given N pairs of systems. Alice generates the random bits $\mathbf{I} = (I_1, \ldots, I_N)$ independently and with identical distribution: $P_I(0) = 1 - \delta, P_I(1) = \delta$, for a small $\delta > 0$. Analogously, Bob generates the random bits $\mathbf{J} = (J_1, \ldots, J_N)$ independently and with identical distribution $P_J = P_I$. Pairs such that $I_n = J_n = 0$ are used to generate the raw key, and pairs such that $I_n = J_n = 1$ are used to estimate how much nonlocality Alice and Bob share. For each $n \in \{1, \ldots, N\}$, if $I_n = 0$ Alice measures her n^{th} system with $X_n = 0$, if $I_n = 1$ she measures it

with X_n chosen uniformly on $\{0,\dots,M-1\}$, if $J_n=0$ Bob measures his n^{th} system with $Y_n=M$, if $J_n=1$ he measures it with Y_n chosen uniformly on $\{0,\dots,M-1\}$.

2. Estimation of nonlocality. They publish $\mathbf{I},\mathbf{J}$ and for the pairs n such that $I_n=J_n=1$ they publish the outcomes (A_n,B_n,X_n,Y_n). The subset of those pairs such that

$$Y_n=X_n \quad \text{or} \quad Y_n=X_n+1 \bmod M \tag{12}$$

is denoted by $\mathcal{N}_{\text{e}}$. With those pairs they compute the average value for the BC-inequality

$$\mathcal{B}_{\text{est}}=\frac{1}{|\mathcal{N}_{\text{e}}|}\sum_{n\in\mathcal{N}_{\text{e}}}\mathcal{B}_n\ , \tag{13}$$

where $\mathcal{B}_n=\mathcal{B}[A_n,B_n,X_n,Y_n]$ is defined in (3). The number of estimated systems is $N_{\text{e}}=|\mathcal{N}_{\text{e}}|\approx 2N\delta^2/M$ with high probability. Here and in the rest of the paper the symbol $\approx$ denotes equality up to subleading terms. As we will see, the asymptotic efficiency of the protocol does not depend on the subleading terms. The outcomes of the systems with $I_n=J_n=0$, which have not been published, are denoted by $A_{\text{r}},B_{\text{r}}$. These are the two versions of the raw key, and we denote their length by N_{r}.

3. Error correction. Alice publishes N_{c} bits of information about the raw key $C=f(\mathbf{A}_{\text{r}})$, which Bob uses in order to correct the errors in his raw key: $\mathbf{B}_{\text{r}}\to\mathbf{B}'_{\text{r}}\approx\mathbf{A}_{\text{r}}$. Any error-correction method can be inserted here, as long as the probability that $\mathbf{B}'_{\text{r}}\neq\mathbf{A}_{\text{r}}$ vanishes as N grows.

4. Privacy amplification. Alice generates and publishes the two-universal random function $G:\{0,1\}^{N_{\text{r}}}\to\{0,1\}^{N_{\text{s}}}$ (see Definition 8 or [18]) with output length

$$N_{\text{s}}\approx N_{\text{r}}2\log_2\frac{1}{\sqrt{2}\,\mathcal{B}_{\text{est}}}-N_{\text{c}} \tag{14}$$

(see Definition 8). Alice and Bob respectively compute $G(\mathbf{A}_{\text{r}})$ and $G(\mathbf{B}'_{\text{r}})$, which constitute their corresponding versions of the final secret key.

IV. UNIVERSALLY-COMPOSABLE SECURITY

We consider the strongest notion of security [13–15], where the eavesdropper is totally unconstrained (apart from no-signaling). In particular, she can use nonclassical systems to store information for an indefinitely long time, and measure them with observables depending on the messages published during the protocol. But even more than this. It is usually the case that the product of a key distribution protocol, the secret key, is used as an ingredient for other protocols. If messages are published during this concatenated protocols, Eve could wait, and choose the observable depending on these later messages. We demand that the security of any task which uses our key distribution protocol as a subroutine is not compromised by the fact that Eve can wait indefinitely for measuring her systems.

All the published information which is potentially correlated to the secret key $K=G(\mathbf{A}_{\text{r}})$ is:

1. the messages that the honest parties publish in order to estimate $\mathcal{B}_{\text{est}}$, denoted D,
2. Alice's message in the error correction step $C=f(\mathbf{A}_{\text{r}})$,
3. the function G.

In this context we define an *ideal secret key* as

$$P^{\text{ideal}}_{K,C,E,D,G|Z}=P_U P_{C,E,D,G|Z} \tag{15}$$

where U is uniform on $\{0,1\}^{N_{\text{s}}}$. The *actual secret key* generated by the protocol is not shown to be an ideal key. Instead we demand the following

Security definition: *the actual secret key must be indistinguishable from an ideal secret key.*

This has to be understood in the strongest sense, where joint measurements on all systems involved in $P_{K,C,E,D|Z}$ are allowed. In other words, even if Alice and Eve bring their systems together and cooperate for discriminating between the actual and the ideal distributions, this task is impossible. Because processing information does not make two states more distinguishable, in any context where the ideal key is secure the actual key is secure too. In Theorem 11 it is shown that

$$\sum_{k,c,g}\max_z\sum_e\Big|P_{K,C,E,G|Z}(k,c,e,g,z)- \\ -\ 2^{-N_{\text{s}}}P_{C,E,G|Z}(c,e,g,z)\Big|\ \le\ \sqrt{2}^{\,-\sqrt{N_{\text{e}}}} \tag{16}$$

holds with probability larger than $1-3Ne^{-\sqrt{N_{\text{e}}}(3M)^{-2}}$. This ensures that the actual and the ideal keys are indistinguishable (see discussion in [15]). Recall that z parametrizes all possible observables that can be measured in Eve's system.

V. EFFICIENCY OF THE PROTOCOL

The efficiency of a key distribution scheme is quantified by the asymptotic secret key rate. This is defined as the ratio N_{s}/N in the limit $N\to\infty$, where N_{s} is the number of perfect secret bits obtained and N is the number of pairs of systems consumed. The number δ, defined in the first step of the protocol, is a free parameter. Choosing $\delta=N^{-1/4}$ gives $N_{\text{e}}\approx 2\sqrt{N}/M$, which ensures security (16) as the number of systems consumed grows ($N\to\infty$). Bob's errors can be corrected if the bit string $C=f(\mathbf{A}_{\text{r}})$ has length

$$N_{\text{c}}\approx N_{\text{r}}\,h(w)\ , \tag{17}$$

where h is the binary Shannon entropy

$$h(w)=-w\log_2 w-(1-w)\log_2(1-w)\ , \tag{18}$$

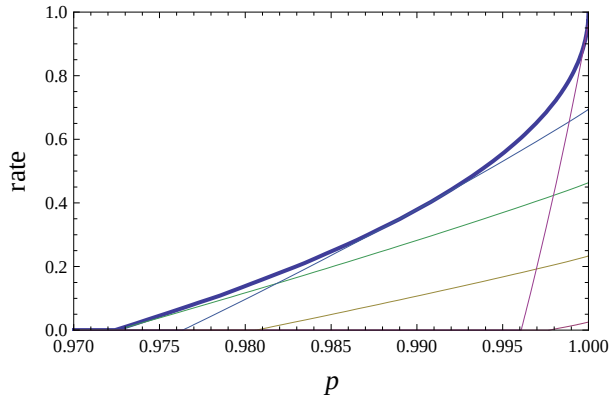

FIG. 2: The secret key rate is plotted versus p. The thin lines correspond to the rates for $M = 3, 4, 6, 11, 100$. One can identify the curves by noting that for $p = 1$ the rate is monotonically increasing with M. The thick line corresponds to the rate optimized over M at each value of p.

and w is the relative frequency of errors ($B_n \neq A_n$). This gives an asymptotic secret key rate of

$$\lim_{N\mapsto\infty} \frac{N_{\rm s}}{N} \;=\; 2\log_2 \frac{1}{\sqrt{2}\,\mathcal{B}_{\rm est}} - h(w)\;. \qquad (19)$$

Let us apply this rate formula to the correlations obtained when measuring the state (8) with the observables (9), (10), (11). For large N, the estimated information tends to

$$\mathcal{B}_{\rm est} \;=\; \frac{1}{2} + M\left(p\,\sin^2\Big[\frac{\pi}{4M}\Big] + \frac{1-p}{2}\right)\;, \qquad (20)$$

$$w \;=\; \frac{1-p}{2}\;, \qquad (21)$$

with high probability. Substituting this into (19) gives the rates plotted in FIG. 2. The rate for $M = 2$ is zero, hence we do not provide a security proof for the CHSH-protocol [9]. For $M = 3$ the rate is non-zero at high p, but quite small. For $M = 6$ the protocol tolerates the maximum level of noise ($p_{\rm min} = .972$). Each amount of noise p has an optimal number of observables M which maximizes the rate. In the noiseless limit $p \to 1$ the optimal M tends to infinite $M \to \infty$.

VI. SECURITY PROOF

A. Properties of symmetric distributions

The results derived in this subsection are relevant on their own. They provide tools for estimating properties of symmetric distributions without resorting to any de Finetti-like theorem. We use calligraphic letter $\mathcal{V}$ to denote the alphabet of values for the corresponding random variable V, that is $v \in \mathcal{V}$.

Definition 1 *Given a string* $\mathbf{v} = (v_1, \ldots, v_N) \in \mathcal{V}^N$ *we define its corresponding frequency* $q = \mathrm{freq}(\mathbf{v})$ *as*

$$q(v) = \frac{\text{times } v \text{ appears in } \mathbf{v}}{N}\;, \quad \forall\, v \in \mathcal{V}\;. \qquad (22)$$

This function is naturally extended to sets $\mathcal{Q} = \mathrm{freq}(\mathcal{V}^N)$, *and random variables* $Q = \mathrm{freq}(\mathbf{V})$.

For any $\mathbf{v}$, the frequency $q = \mathrm{freq}(\mathbf{v})$ is a probability distribution for the random variable V, but it has the specific feature that it only takes values on the set $\{\frac{k}{N} : k = 0, \ldots, N\}$. $\mathcal{Q}$ is the set of all possible frequencies, whose cardinality can be bounded as

$$|\mathcal{Q}| \leq (N+1)^{|\mathcal{V}|-1}\;. \qquad (23)$$

For what follows, it is convenient to define a particular kind of probability distributions for $\mathbf{V}$: *the distribution with well-defined frequency* $q \in \mathcal{Q}$, denoted $P_{\mathbf{V}|q}$, is the uniform distribution over all strings $\mathbf{v} \in \mathcal{V}^N$ such that $\mathrm{freq}(\mathbf{v}) = q$. Another important kind of symmetric distributions are the *i.i.d. distributions*, representing independent and identically-distributed random variables $V_1, \ldots, V_N$. A distribution $P_{\mathbf{V}}$ is i.i.d. if there exists a single-copy distribution P_V such that $P_{\mathbf{V}} = (P_V)^{\otimes N}$. If $P_V(v) < 1$ for all v, then the i.i.d. distribution $(P_V)^{\otimes N}$ has not a well-defined frequency. Hence, not all symmetric distributions have a well-defined frequency. However, any symmetric distribution $P^{\rm sym}_{\mathbf{V}}$ can be written as a mixture of distributions with well-defined frequency,

$$P^{\rm sym}_{\mathbf{V}} = \sum_{q\in\mathcal{Q}} P_Q(q)\, P_{\mathbf{V}|q}\;, \qquad (24)$$

where $Q = \mathrm{freq}(\mathbf{V})$. These two equalities establish a one-to-one correspondence between Q and $\mathbf{V}$, for symmetric distributions. In the following lemma we show that, in a sense, general symmetric distributions are similar to i.i.d. distributions. This result is motivated by the ideas presented in [16].

Lemma 2 *If there is an event* $\mathcal{E} \subseteq \mathcal{V}^N$ *and* $\epsilon > 0$ *such that for any (single-copy) distribution* P_V *the bound* $(P_V)^{\otimes N}(\mathcal{E}) \leq \epsilon$ *holds, then for any symmetric distribution* $P^{\rm sym}_{\mathbf{V}}$ *we have*

$$P^{\rm sym}_{\mathbf{V}}(\mathcal{E}) \leq \epsilon\,|\mathcal{Q}|\;. \qquad (25)$$

Proof Let us first prove (25) for distributions with well-defined frequency, that is

$$P_{\mathbf{V}|q}(\mathcal{E}) \leq \epsilon\,|\mathcal{Q}|\,, \quad \forall\, q \in \mathcal{Q}\;. \qquad (26)$$

For any $q' \in \mathcal{Q}$ we can apply the premise of the lemma: $(q')^{\otimes N}(\mathcal{E}) \leq \epsilon$. Using the decomposition (24), we know that there is a random variable Q' such that $\sum_{q\in\mathcal{Q}} P_{Q'}(q)\, P_{\mathbf{V}|q} = (q')^{\otimes N}$, and then

$$\sum_{q\in\mathcal{Q}} P_{Q'}(q) P_{\mathbf{V}|q}(\mathcal{E}) \leq \epsilon\;. \qquad (27)$$

In Lemma 3 it is shown that the distribution $P_{Q'}(q)$ reaches the maximum at $q = q'$, which implies $P_{Q'}(q') \geq 1/|\mathcal{Q}|$. Then

$$P_{\mathbf{V}|q'}(\mathcal{E}) \;\leq\; |\mathcal{Q}|\, P_{Q'}(q')\, P_{\mathbf{V}|q'}(\mathcal{E}) \;\leq\; |\mathcal{Q}|\,\epsilon\ ,$$

where the last inequality follows from (27). Finally, we prove (25) by applying the bound (26) to each term in (24). □

Lemma 3 *Let the probability distribution P_V take values on the set $\{\frac{k}{N} : k = 0, \ldots, N\}$, and let $\mathbf{V} = (V_1, \ldots, V_N)$ be distributed according to $(P_V)^{\otimes N}$. Then the probability distribution P_Q for $Q = \mathrm{freq}(\mathbf{V})$ takes its maximum at $Q = P_V$, that is,*

$$P_Q(P_V) = \max_{q\in\mathcal{Q}} P_Q(q)\ . \tag{28}$$

Proof We show that for any $q \in \mathcal{Q}$ with $q \neq P_V$ there exists $q' \in \mathcal{Q}$ such that $P_Q(q') > P_Q(q)$. Let thus $q \in \mathcal{Q}$ be fixed such that $q \neq P_V$. We call the *support* of q: the set of values v such that $q(v) > 0$. If the support of q is not contained in the support of P_V then $P_Q(q) = 0$. We can thus without loss of generality assume that the alphabet of V, denoted $\mathcal{V}$, is the support of P_V, that is, $P_V(v) > 0$ for all $v \in \mathcal{V}$. For any $v \in \mathcal{V}$ define

$$d(v) = q(v) - P_V(v)\ .$$

Furthermore, let $v_{\min}$ and $v_{\max}$ be defined by

$$\begin{array}{l} d(v_{\min}) = \min_v d(v) \\ d(v_{\max}) = \max_v d(v) \end{array}\ .$$

Because $q \neq P_V$ and the assumption of the lemma, $d(v_{\min}) \leq -1/N$ and $d(v_{\max}) \geq 1/N$. Let us define $q' \in \mathcal{Q}$ as

$$q'(v) = \begin{cases} q(v) + \frac{1}{N} & \text{if } v = v_{\min} \\ q(v) - \frac{1}{N} & \text{if } v = v_{\max} \\ q(v) & \text{otherwise.} \end{cases}$$

From the two inequalities above we have

$$\begin{array}{l} q'(v_{\min}) \leq P_V(v_{\min}) \\ q'(v_{\max}) \geq P_V(v_{\max}) \end{array}\ . \tag{29}$$

Using the identity

$$P_Q(q) = \frac{N! \prod_v P_V(v)^{q(v)N}}{\prod_v (q(v)N)!}$$

we find

$$\frac{P_Q(q')}{P_Q(q)} = \frac{P_V(v_{\min})(q'(v_{\max}) + \frac{1}{N})}{P_V(v_{\max}) q'(v_{\min})} > \frac{P_V(v_{\min})}{P_V(v_{\max})} \frac{q'(v_{\max})}{q'(v_{\min})}$$

(note that the terms in the denominator cannot be zero). By (29), the right-hand side cannot be smaller than 1, which concludes the proof. □

Lemma 4 (Bernstein's inequality) *If $V_1, \ldots, V_N$ are i.i.d. random variables then*

$$\mathrm{prob}\Big\{|V_1 + \cdots + V_N - N\langle V\rangle| > \omega\sqrt{\langle V^2\rangle N}\Big\} < 2\, e^{-\omega^2/4}$$

where $\langle V\rangle$ and $\langle V^2\rangle$ are the first and second moment, and $\omega > 0$.

Lemma 5 *Let $V_1, \ldots, V_N$ be symmetrically-distributed random variables over the finite alphabet $\mathcal{V}$, and $v_+ = \max\{|v|; v \in \mathcal{V}\}$. Let N_1, N_2 be positive integers such that $N_1 + N_2 = N$. The random variable*

$$V_{\mathrm{est}} = \frac{1}{N_2} \sum_{n=N_1+1}^{N} V_n \tag{30}$$

satisfies

$$\begin{aligned} &\mathrm{prob}\Big\{\langle V_1 \cdots V_{N_1}\rangle \leq \Big(V_{\mathrm{est}} + N_2^{-1/4}\Big)^{N_1}\Big\} \\ &\geq\ 1 - 2\,|\mathcal{Q}| \exp\Big(-\frac{\sqrt{N_2}}{4\, v_+^2}\Big)\ . \end{aligned} \tag{31}$$

Proof Let us first show (31) for $V_1, \ldots, V_N$ being i.i.d. In this case

$$\langle V_1 \cdots V_{N_1}\rangle = \langle V\rangle^{N_1}\ . \tag{32}$$

Also, one can apply Bernstein's inequality (Lemma 4) to the sum (30) as

$$\mathrm{prob}\Big\{V_{\mathrm{est}} < \langle V\rangle - N_2^{-1/4}\Big\} < 2\exp\Big(-\frac{\sqrt{N_2}}{4\,\langle V^2\rangle}\Big)$$

with $\omega = N_2^{1/4}\langle V^2\rangle^{-1/2}$. This, equation (32), and inequality $\langle V^2\rangle \leq v_+^2$ imply

$$\begin{aligned} &\mathrm{prob}\Big\{\langle V_1 \cdots V_{N_1}\rangle > \Big(V_{\mathrm{est}} + N_2^{-1/4}\Big)^{N_1}\Big\} \\ &<\ 2\exp\Big(-\frac{\sqrt{N_2}}{4\, v_+^2}\Big)\ . \end{aligned}$$

Lemma 2 states that if the above holds for any i.i.d. distribution, the following holds for any symmetric distribution

$$\begin{aligned} &\mathrm{prob}\Big\{\langle V_1 \cdots V_{N_1}\rangle > \Big(V_{\mathrm{est}} + N_2^{-1/4}\Big)^{N_1}\Big\} \\ &<\ 2\,|\mathcal{Q}| \exp\Big(-\frac{\sqrt{N_2}}{4\, v_+^2}\Big)\ . \end{aligned}$$

From here, inequality (31) is immediate. □

B. Properties of nonsignlaing distributions

Let us introduce some notation. We represent single-pair distributions $P_{A,B|X,Y}$ as vectors with components

arranged in the following way

$$P_{A,B|X,Y} = \tag{33}$$

$P(0,0\|0,0)$ $P(0,1\|0,0)$ $P(1,0\|0,0)$ $P(1,1\|0,0)$	$\ldots$	$P(0,0\|0,M-1)$
$\vdots$	$\ddots$	$\vdots$
$P(0,0\|M-1,0)$	$\ldots$	$P(0,0\|M-1,M-1)$

Define the following two vectors (which are not probability distributions)

$$\mu = \frac{1}{4M} \begin{array}{|cc|cc|c|c|} \hline 1&1&1&1&&\\ 1&1&1&1&&\\ \hline &&1&1&\ddots&\\ &&1&1&&\\ \hline &&&&\ddots&1\ 1\\ &&&&&1\ 1\\ \hline 1&1&&&&1\ 1\\ 1&1&&&&1\ 1\\ \hline \end{array} , \tag{34}$$

$$\nu = \frac{1}{2} \begin{array}{|cc|cc|c|c|} \hline 0&1&0&1&&\\ -1&0&-1&0&&\\ \hline &&0&-1&\ddots&\\ &&1&0&&\\ \hline &&&&\ddots&0\ 1\\ &&&&&-1\ 0\\ \hline 1&0&&&&0\ -1\\ 0&-1&&&&1\ 0\\ \hline \end{array} , \tag{35}$$

where empty boxes have to be understood as having zeros

$$\boxed{} = \boxed{\begin{matrix}0&0\\0&0\end{matrix}} , \tag{36}$$

and ellipsis between two identical boxes have to be understood as an arbitrarily large sequence of identical boxes. From now on, the absolute value of a vector means component-wise absolute value. For example

$$|\nu| = \frac{1}{2} \begin{array}{|cc|cc|c|c|} \hline 0&1&0&1&&\\ 1&0&1&0&&\\ \hline &&0&1&\ddots&\\ &&1&0&&\\ \hline &&&&\ddots&0\ 1\\ &&&&&1\ 0\\ \hline 1&0&&&&0\ 1\\ 0&1&&&&1\ 0\\ \hline \end{array} .$$

Also, an inequality "$\preceq$" between two vectors means components-wise inequality "$\leq$". For example $\nu \preceq |\nu|$.

Define the vectors

$$\beta_a = \mu + (-1)^a \nu , \tag{37}$$

$$\beta = \mu + |\nu| . \tag{38}$$

One can check that the Braunstein-Caves Bell inequality, defined in (3), can be written as

$$\langle \mathcal{B} \rangle = \beta \cdot P_{A,B|X,Y} . \tag{39}$$

Lemma 6 *If $P_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y}}$ is an arbitrary $2N$-partite nonsignaling distribution then for any* $\mathbf{a}$

$$P_{\mathbf{A}|\mathbf{X}}(\mathbf{a},\mathbf{0}) = \left(\bigotimes_{n=1}^{N} \beta_{a_n} \right) \cdot P_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y}} , \tag{40}$$

where $\mathbf{0} = (0,\ldots,0)$.

Proof: Let us first consider the bound (40) for one pair of systems ($N = 1$). The no-signaling constraint $P_{A|X,Y}(0,0,0) = P_{A|X,Y}(0,0,1)$ can also be expressed as the scalar product

$$\begin{array}{|cc|cc|c|c|} \hline -1&-1&1&1&&\\ &&&&&\\ \hline &&&&\ddots&\ddots\\ &&&&&\\ \hline \end{array} \cdot P_{A,B|X,Y} = 0$$

and the no-signaling constraint $P_{B|X,Y}(0,0,0) = P_{B|X,Y}(0,M-1,0)$ can be expressed as

$$\begin{array}{|c|c|c|c|} \hline -1&&&\\ -1&&&\\ \hline &&\ddots&\\ &&&\\ \hline &&\ddots&\\ &&&\\ \hline 1&&&\\ 1&&&\\ \hline \end{array} \cdot P_{A,B|X,Y} = 0 .$$

The remaining no-signaling constraints can be written in an analogous fashion. A linear combination of those equalities gives

$$\begin{array}{|cc|cc|c|c|} \hline 1&1&1&1&&\\ 1&1&1&1&&\\ \hline &&1&1&\ddots&\\ &&1&1&&\\ \hline &&&&\ddots&1\ 1\\ &&&&&1\ 1\\ \hline \tau_-&\tau_-&&&&1\ 1\\ \tau_-&\tau_-&&&&1\ 1\\ \hline \end{array} \cdot P_{A,B|X,Y} = 0 , \tag{41}$$

where $\tau_- = 1 - 2M$. If $P_{A,B|X,Y}$ is a nonsignaling distribution, the following equalities hold.

$$P_{A|X}(0,0) = \begin{array}{|c|c|c|c|}\hline 1\quad 1 & & & \\ \hline & & \ddots & \\ \hline & & \ddots & \\ \hline & & & \\ \hline\end{array} \cdot P_{A,B|X,Y}$$

$$= \frac{1}{2} \begin{array}{|c|c|c|c|}\hline 1\quad 1 & \quad 1 \\ & -1 & & \\ \hline & 1 & \ddots & \\ & 1 & & \\ \hline & & \ddots & \\ \hline & & & \\ \hline\end{array} \cdot P_{A,B|X,Y}$$

$$= \frac{1}{2} \begin{array}{|c|c|c|c|}\hline \quad 1 & \quad 1 & & \\ -1 & -1 & & \\ \hline & \quad -1 & \ddots & \\ & 1 & & \\ \hline & & \ddots & \quad 1 \\ & & & -1 \\ \hline 2\quad 1 & & & \quad -1 \\ 1 & & & 1 \\ \hline\end{array} \cdot P_{A,B|X,Y}$$

The second and third equalities follow by adding linear combinations of nonsignaling constraints. The above plus (41) times $1/4M$ gives

$$P_{A|X}(0,0) = (\mu + \nu) \cdot P_{A,B|X,Y} \ .$$

Under the relabeling

$$(A, B) \to (A \oplus 1, B \oplus 1) \ ,$$

we have the transformations

$$\begin{aligned} P_{A|X}(0,0) &\to P_{A|X}(1,0) \ , \\ \mu &\to \mu \ , \\ \nu &\to -\nu \ , \end{aligned}$$

which imply $P_{A|X}(a,0) = \beta_a \cdot P_{A,B|X,Y}$. The generalization to N pairs of systems is straightforward. Each no-signaling constraint involves a linear combination of the entries of $P_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y}}$ where all indexes remain constant except the ones corresponding to one system (like for instance a_1, x_1). Hence we can apply the above argument to each of the N pairs separately, obtaining (40). □

The following lemma is not necessary for the security proof. We include it because it provides insight on the trade-off between Bell-inequality violation and correlation with a third party —the monogamy of nonlocal correlations. This is explained around equation (7). If, in addition to no-signaling, one also assumes the validity of quantum theory, the following lemma together with [17] is enough to establish the security of privacy amplification, and provides a larger efficiency rate

Lemma 7 *Let $P_{\mathbf{A},\mathbf{B},E|\mathbf{X},\mathbf{Y},Z}$ be an arbitrary $(2N+1)$-partite nonsignaling distribution and define*

$$\begin{aligned} &\mathcal{P}_{\text{guess}}(\mathbf{A}|E,\mathbf{x}) \qquad (42) \\ &\quad = \max_z \sum_e P_{E|Z}(e,z) \max_{\mathbf{a}} P_{\mathbf{A}|\mathbf{X},E,Z}(\mathbf{a},\mathbf{x},e,z) \ . \end{aligned}$$

For any $\mathbf{x}$ we have

$$\mathcal{P}_{\text{guess}}(\mathbf{A}|E,\mathbf{x}) \leq \ \langle \mathcal{B}_1 \cdots \mathcal{B}_N \rangle \ , \qquad (43)$$

where $\mathcal{B}_n = \mathcal{B}[A_n, B_n, X_n, Y_n]$ and $\mathcal{B}$ is defined by (3).

Proof: Using the no-signaling condition we can write

$$P_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y}} = \sum_e P_{E|Z}(e,z) \, P_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y},E,Z}(e,z) \ . \qquad (44)$$

Let us show that

$$\beta_{a_1} \otimes \cdots \otimes \beta_{a_n} \preceq \beta^{\otimes n} \ , \qquad (45)$$

for any n and any $(a_1, \ldots, a_n) \in \{0,1\}^n$. First, expand each side of this inequality according to definitions (37) and (38); second, note that $\mp\nu^{\otimes n} \preceq |\nu^{\otimes n}| = |\nu|^{\otimes n}$; and finally, use this to show that each term in the left is component-wise bounded by the corresponding term in the right. Let us show (43) for the case $\mathbf{x} = (0, \ldots, 0)$. In the following chain of equalities and inequalities we use, respectively: the definition of $\mathcal{P}_{\text{guess}}$ in (42); Lemma 6; inequality (45) and positivity of the vectors $P_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y},E,Z}(e,z)$; the linearity of the scalar product; decomposition (44); and the identity (39).

$$\begin{aligned} & \mathcal{P}_{\text{guess}}(\mathbf{A}|E,\mathbf{x}) \\ = \ & \max_z \sum_e P_{E|Z}(e,z) \max_{\mathbf{a}} P_{\mathbf{A}|\mathbf{X},E,Z}(\mathbf{a},\mathbf{x},e,z) \\ = \ & \max_z \sum_e P_{E|Z}(e,z) \max_{\mathbf{a}} \left(\bigotimes_{n=1}^{N} \beta_{a_n} \right) \cdot P_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y},E,Z}(e,z) \\ \leq \ & \max_z \sum_e P_{E|Z}(e,z) \, \beta^{\otimes N} \cdot P_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y},E,Z}(e,z) \\ = \ & \max_z \beta^{\otimes N} \cdot \left(\sum_e P_{E|Z}(e,z) P_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y},E,Z}(e,z) \right) \\ = \ & \beta^{\otimes N} \cdot P_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y}} \\ = \ & \langle \mathcal{B}_1 \cdots \mathcal{B}_N \rangle \end{aligned}$$

In order to extend this inequality to all values of $\mathbf{x}$, consider the relabeling. For any $m \in \{0, \ldots, M-1\}$

$$\begin{array}{rcl} X & \to & X + m \bmod M \\ Y & \to & Y + m \bmod M \\ A & \to & A \oplus I\{M-m \le X \le M-1\} \\ B & \to & B \oplus I\{M-m \le Y \le M-1\} \end{array} . \tag{46}$$

This relabeling corresponds to a permutation of the entries of the vectors (33) such that

$$P_{A|X}(a,0) \to P_{A|X}(a,m) .$$

This relabeling leaves the vector β invariant. Hence, performing the relabeling to each pair with $m = x_n$, the above inequality for $\mathbf{x} = (0, \ldots, 0)$ is generalized to any value of $\mathbf{x}$. □

C. Privacy amplification

This privacy amplification scheme is similar to the one introduced in [15]. It has the advantage that one can hash out any information about the raw key $C = f(\mathbf{A})$, that is, the function f is arbitrary. Contrary, the scheme introduced in [15] only works when the function f is generic. Our privacy amplification scheme has the disadvantage that it needs a random hash function G, in particular a two-universal one [18], while the one in [15] works with a deterministic hash function.

Definition 8 *A random function $G : \{0,1\}^N \to \{0,1\}^{N_s}$ is called two-universal [18] if for any pair $\mathbf{a}, \mathbf{a}' \in \{0,1\}^N$ such that $\mathbf{a} \neq \mathbf{a}'$ we have*

$$\mathrm{prob}\{G(\mathbf{a}) = G(\mathbf{a}')\} \le 2^{-N_s} . \tag{47}$$

Lemma 9 *If $G : \{0,1\}^N \to \{0,1\}^{N_s}$ is a two-universal random function, then for any subset $\mathcal{A} \subseteq \{0,1\}^N$ we have*

$$\sum_{k,g} P_G(g) \Big| \sum_{\mathbf{a}\in\mathcal{A}} \big(\delta^k_{g(\mathbf{a})} - 2^{-N_s}\big) \Big| \le \sqrt{2^{N_s}|\mathcal{A}|} , \tag{48}$$

where k runs over $\{0,1\}^{N_s}$.

Proof In what follows we take the square of the left-hand side of (48); use the convexity of the square function; sum over k; partially sum over $\mathbf{a}, \mathbf{a}', g$; use the two-universality of G; and a trivial bound.

$$\begin{aligned} & \Big(\sum_{k,g} P_G(g) \Big| \sum_{\mathbf{a}\in\mathcal{A}} \big(\delta^k_{g(\mathbf{a})} - 2^{-N_s}\big) \Big| \Big)^2 \\ \le & \sum_{k,g} 2^{-N_s} P_G(g) \sum_{\mathbf{a},\mathbf{a}'\in\mathcal{A}} \Big(2^{2N_s} \delta^k_{g(\mathbf{a})} \delta^k_{g(\mathbf{a}')} + 1 - 2^{1+N_s} \delta^k_{g(\mathbf{a})} \Big) \\ = & \sum_{g} P_G(g) \sum_{\mathbf{a},\mathbf{a}'\in\mathcal{A}} \Big(2^{N_s}\, \delta^{g(\mathbf{a})}_{g(\mathbf{a}')} - 1 \Big) \\ = & \; 2^{N_s} \sum_{\mathbf{a},\mathbf{a}'\in\mathcal{A}:\, \mathbf{a}\neq\mathbf{a}'} \Big(\sum_g P_G(g)\, \delta^{g(\mathbf{a})}_{g(\mathbf{a}')} \Big) + 2^{N_s}|\mathcal{A}| - |\mathcal{A}|^2 \\ \le & \; \big(|\mathcal{A}|^2 - |\mathcal{A}|\big) + 2^{N_s}|\mathcal{A}| - |\mathcal{A}|^2 \\ \le & \; 2^{N_s}|\mathcal{A}| . \end{aligned}$$

□

Theorem 10 *Let $P_{\mathbf{A},\mathbf{B},E|\mathbf{X},\mathbf{Y},Z}$ be a $(2N+1)$-partite nonsignaling distribution, let $C = f(\mathbf{A})$ where $f : \{0,1\}^N \to \{0,1\}^{N_c}$ is a given function, and let $K = g(\mathbf{A})$ where $G : \{0,1\}^N \to \{0,1\}^{N_s}$ a two-universal random function, then*

$$\begin{aligned} & \sum_{k,c,g} \max_z \sum_e \Big| P_{K,C,E,G|\mathbf{X},Z}(k,c,e,g,\mathbf{0},z) - \\ & \quad - 2^{-N_s} P_{C,E,G|\mathbf{X},Z}(c,e,g,\mathbf{0},z) \Big| \\ \le & \; \sqrt{2}^{N+N_s+N_c+1} \big\langle \mathcal{B}_1 \cdots \mathcal{B}_N \big\rangle , \end{aligned} \tag{49}$$

where $\mathcal{B}_n = \mathcal{B}[A_n, B_n, X_n, Y_n]$ and $\mathcal{B}$ is defined in (3).

Proof For any subset $\mathcal{A} \subseteq \{0,1\}^N$ we have the following chain of component-wise inequalities.

$$\begin{aligned} & \sum_{k,g} P_G(g) \Big| \sum_{\mathbf{a}\in\mathcal{A}} \big(\delta^k_{g(\mathbf{a})} - 2^{-N_s}\big) \bigotimes_{n=1}^N \beta_{a_n} \Big| \\ \preceq & \sum_{k,g} P_G(g) \Big(\mu^{\otimes N} \Big| \sum_{\mathbf{a}\in\mathcal{A}} \big(\delta^k_{g(\mathbf{a})} - 2^{-N_s}\big) \Big| + \\ & + |\nu| \otimes \mu^{\otimes N-1} \Big| \sum_{\mathbf{a}\in\mathcal{A}} (-1)^{a_1} \big(\delta^k_{g(\mathbf{a})} - 2^{-N_s}\big) \Big| + \\ & + \cdots + |\nu|^{\otimes N} \Big| \sum_{\mathbf{a}\in\mathcal{A}} (-1)^{a_1+\cdots+a_N} \big(\delta^k_{g(\mathbf{a})} - 2^{-N_s}\big) \Big| \Big) \\ \preceq & \; \mu^{\otimes N} \sqrt{2^{N_s}|\mathcal{A}|} + |\nu| \otimes \mu^{\otimes N-1} \sqrt{2^{1+N_s}|\mathcal{A}|} \\ & + \cdots + |\nu|^{\otimes N} \sqrt{2^{1+N_s}|\mathcal{A}|} \\ \preceq & \; \sqrt{2^{1+N_s}|\mathcal{A}|}\; \beta^{\otimes N} \end{aligned} \tag{50}$$

In the first step we use the expansion

$$\begin{aligned} & \bigotimes_{n=1}^N \beta_{a_n} \\ = & \; \mu^{\otimes N} + (-1)^{a_1} \nu \otimes \mu^{\otimes N} + \cdots + (-1)^{a_1+\cdots+a_N} \nu^{\otimes N} , \end{aligned} \tag{51}$$

and the component-wise triangular inequality. In the second step we use the following triangular inequality for any $\mathbf{u} \in \{0,1\}^N$

$$\begin{aligned} &\Big| \sum_{\mathbf{a}\in\mathcal{A}} (-1)^{\mathbf{a}\cdot\mathbf{u}} \big(\delta^k_{g(\mathbf{a})} - 2^{-N_{\rm s}}\big) \Big| \\ \leq\ & \Big| \sum_{\mathbf{a}\in\mathcal{A}:\, \mathbf{a}\cdot\mathbf{u}=0 \bmod 2} \big(\delta^k_{g(\mathbf{a})} - 2^{-N_{\rm s}}\big) \Big| \\ &+ \Big| \sum_{\mathbf{a}\in\mathcal{A}:\, \mathbf{a}\cdot\mathbf{u}=1 \bmod 2} \big(\delta^k_{g(\mathbf{a})} - 2^{-N_{\rm s}}\big) \Big| \ , \end{aligned}$$

Lemma 9, and the concavity of the square-root function

$$\sum_{i=1}^M \sqrt{t_i} \leq \sqrt{M \sum_{i=1}^M t_i} \ . \tag{52}$$

For the last inequality all terms are summed up by using $\beta = \mu + |\nu|$.

In the rest of this proof the following notation is used. We denote by $P_{\mathbf{A},\mathbf{B},e|\mathbf{X},\mathbf{Y},z} = P_{\mathbf{A},\mathbf{B},E|\mathbf{X},\mathbf{Y},Z}(e,z)$ the vector with entries $P_{\mathbf{A},\mathbf{B},E|\mathbf{X},\mathbf{Y},Z}(\mathbf{a},\mathbf{b},e,\mathbf{x},\mathbf{y},z)$ for all values of $\mathbf{a},\mathbf{b},\mathbf{x},\mathbf{y}$ and fixed values of e,z. Following this notation we can write $P_{\mathbf{a}} = P_{\mathbf{A}}(\mathbf{a})$. For any subsets $\mathcal{A} \subseteq \{0,1\}^N$ and any set of coefficients $\eta_{\mathbf{a}}$ we have the following chain of equalities and inequalities,

$$\begin{aligned} &\sum_e P_{e|z} \Big| \sum_{\mathbf{a}\in\mathcal{A}} \eta_{\mathbf{a}}\, P_{\mathbf{a}|e,z} \Big| \\ =\ & \sum_e P_{e|z} \Big| \sum_{\mathbf{a}\in\mathcal{A}} \eta_{\mathbf{a}} \bigotimes_{n=1}^N \beta_{a_n} \cdot P_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y},e,z} \Big| \\ \leq\ & \sum_e P_{e|z} \Big| \sum_{\mathbf{a}\in\mathcal{A}} \eta_{\mathbf{a}} \bigotimes_{n=1}^N \beta_{a_n} \Big| \cdot P_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y},e,z} \\ =\ & \Big| \sum_{\mathbf{a}\in\mathcal{A}} \eta_{\mathbf{a}} \bigotimes_{n=1}^N \beta_{a_n} \Big| \cdot \sum_e P_{e|z}\, P_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y},e,z} \\ =\ & \Big| \sum_{\mathbf{a}\in\mathcal{A}} \eta_{\mathbf{a}} \bigotimes_{n=1}^N \beta_{a_n} \Big| \cdot P_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y}} \ , \end{aligned} \tag{53}$$

where we have respectively used: Lemma 6, the Cauchy-Schwarz inequality, the linearity of the scalar product, and the definition of the conditional distribution. The following establishes (49).

$$\begin{aligned} &\sum_{k,c,g} \max_z \sum_e \Big| P_{k,c,g,e|z} - 2^{-N_{\rm s}} P_{c,g,e|z} \Big| \\ =\ & \sum_{k,c,g} \max_z \sum_e P_{g,e|z} \Big| P_{k,c|g,e,z} - 2^{-N_{\rm s}} P_{c|e,z} \Big| \\ =\ & \sum_{k,c,g} \max_z \sum_e P_{g,e|z} \Big| \sum_{\mathbf{a}\in f^{-1}(c)} \big(\delta^k_{g(\mathbf{a})} - 2^{-N_{\rm s}}\big) P_{\mathbf{a}|e,z} \Big| \\ \leq\ & \sum_{k,c,g} P_g \Big| \sum_{\mathbf{a}\in f^{-1}(c)} \big(\delta^k_{g(\mathbf{a})} - 2^{-N_{\rm s}}\big) \bigotimes_{n=1}^N \beta_{a_n} \Big| \cdot P_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y}} \\ \leq\ & \sum_c \sqrt{2^{1+N_{\rm s}} |f^{-1}(c)|}\ \beta^{\otimes N} \cdot P_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y}} \\ \leq\ & \sqrt{2^{1+N_{\rm s}+N_{\rm c}+N}}\, \beta^{\otimes N} \cdot P_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y}} \ , \end{aligned} \tag{54}$$

In the above we have respectively used: the definition of conditional distribution; equality $P_c = \sum_{\mathbf{a}\in f^{-1}(c)} P_{\mathbf{a}}$; inequality (53) with $\mathcal{A} = f^{-1}(c)$; the component-wise inequality (50) together with the fact that the components of the vector $P_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y}}$ are positive; and the last inequality follows from (52) and $\sum_c |f^{-1}(c)| = 2^N$. □

D. Security from estimated information

According to the previous theorem, the security of the secret key can be bounded in terms of the quantity $\langle \mathcal{B}_1 \cdots \mathcal{B}_N \rangle$, which does not depend on E at all! This is a particular manifestation of the monogamy of nonlocal correlations. In the unconditional-security scenario Alice and Bob do not know the distribution $P_{\mathbf{A}_{\rm r},\mathbf{B}_{\rm r}|\mathbf{X}_{\rm r},\mathbf{Y}_{\rm r}}$, hence, how can they estimate $\langle \mathcal{B}_1 \cdots \mathcal{B}_N \rangle$? The only thing they know is the estimated information $\mathcal{B}_{\rm est}$, defined in (13). The following result establishes the security of the secret key in terms of $\mathcal{B}_{\rm est}$.

Theorem 11 *Let $P_{\mathbf{A},\mathbf{B},E|\mathbf{X},\mathbf{Y},Z}$ be a $(2N+1)$-partite nonsignaling distribution whose marginal $P_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y}}$ is symmetric with respect to the N 4-component variables (A_n, B_n, X_n, Y_n). Suppose the first $N_{\rm r}$ systems of Alice are measured with $X = 0$, obtaining the outcomes $\mathbf{A}_{\rm r} = (A_1, \ldots, A_{N_{\rm r}})$. Suppose the last $N_{\rm e} = N - N_{\rm r}$ pairs are measured with (X_n, Y_n) chosen uniformly on $\{(x,y) : y = x \text{ or } y = x+1 \bmod M\}$, and let*

$$\mathcal{B}_{\rm est} = \frac{1}{N_{\rm e}} \sum_{n=N_{\rm r}+1}^N \mathcal{B}[A_n, B_n, X_n, Y_n] \ . \tag{55}$$

Let $C = f(\mathbf{A}_{\rm r})$ where $f : \{0,1\}^{N_{\rm r}} \to \{0,1\}^{N_{\rm c}}$ is a given function, and $K = g(\mathbf{A}_{\rm r})$ where $G : \{0,1\}^{N_{\rm r}} \to \{0,1\}^{N_{\rm s}}$ is a two-universal random function with output size

$$N_{\rm s} = N_{\rm r}\, 2 \log_2 \frac{1/\sqrt{2}}{\mathcal{B}_{\rm est} + N_{\rm e}^{-1/4}} - N_{\rm c} - \sqrt{N_{\rm e}} \ . \tag{56}$$

The inequality

$$\sum_{k,c,g} \max_z \sum_e \Big| P_{K,C,E,G|Z}(k,c,e,g,z) - 2^{-N_{\rm s}} P_{C,E,G|Z}(c,e,g,z) \Big| \;\leq\; \sqrt{2}^{-\sqrt{N_{\rm e}}} \qquad (57)$$

holds with probability larger than $1 - 3Ne^{-\sqrt{N_{\rm e}}(3M)^{-2}}$.

Proof Applying Lemma 5 to $\mathcal{B}_{\rm est}$ and $\langle \mathcal{B}_1 \cdots \mathcal{B}_{N_{\rm r}} \rangle$ we conclude that

$$\langle \mathcal{B}_1 \cdots \mathcal{B}_{N_{\rm r}} \rangle \leq \left(\mathcal{B}_{\rm est} + N_{\rm e}^{-1/4} \right)^{N_{\rm r}} \qquad (58)$$

holds with probability larger than

$$\begin{aligned} & 1 - 2(N+1)\exp[-(1+2M)^{-2}\sqrt{N_{\rm e}}] \\ \geq\; & 1 - 3N\exp[-(3M)^{-2}\sqrt{N_{\rm e}}] \; . \end{aligned}$$

For the last, note that the maximum value the variable $\mathcal{B}$ can achieve is $1/2 + M$. Using Theorem 10, inequality (58), and the assignation (56) we obtain

$$\begin{aligned} & \sum_{k,c,g} \max_z \sum_e \Big| P_{K,C,E,G|Z}(k,c,e,g,z) \\ & -2^{-N_{\rm s}} P_{C,E,G|Z}(c,e,g,z) \Big| \\ \leq\; & \sqrt{2}^{N_{\rm r}+N_{\rm s}+N_{\rm c}+1} \left[\mathcal{B}_{\rm est} + N_{\rm e}^{-1/4} \right]^{N_{\rm r}} \\ \leq\; & \sqrt{2}^{-\sqrt{N_{\rm e}}} \; , \end{aligned}$$

which concludes the security proof. □

Now, a few comments are in order.

1. Note that the distribution $P_{\mathbf{A},\mathbf{B},E|\mathbf{X},\mathbf{Y},Z}$ considered in Theorem 11 does not represent all pairs of systems that Alice and Bob share at the beginning of the protocol. It does not include the pairs such that $I_n = J_n = 1$ but do not satisfy condition (12). However, this is irrelevant in establishing the security of the secret key K (see comments below).

2. There is no reason to believe that the honest parties' marginal distribution is symmetric. However, it is measured and processed in a completely symmetric way. For example, the $N_{\rm e}$ pairs used in the estimation of $\mathcal{B}_{\rm est}$ are chosen at random. This is equivalent to the situation considered in Theorem 11, where the distribution is assumed to be symmetric and the pairs used in the estimation constitute a fixed subset.

3. Theorem 11 limits the knowledge that Eve has about the secret key K, even if she hears the messages published in the error correction step $C = f(\mathbf{A}_{\rm r})$. However, the messages published in the estimation of $\mathcal{B}_{\rm est}$, denoted by D in (16), are not considered. The information D is not a function of $\mathbf{A}_{\rm r}$, D is generated by measuring other systems. Therefore, we can consider those systems (the ones used in the estimation), as well as the rest of the universe, as part of Eve's power. Summarizing, the situation considered in Theorem 11 is as complete as required in (16).

VII. CONCLUSIONS

We show that it is possible to generate secret key from correlations that violate the Braunstein-Caves inequality [5] by a sufficient amount. We prove this according to the strongest notion of security, the so-called universally-composable security [13, 14]. The only assumption used in the security proof is the impossibility of arbitrarily-fast signaling between subsystems by performing local measurements.

We introduce an exponentially-accurate scheme for estimating symmetric properties of general distributions. This allows Alice and Bob to treat any unknown given correlations as if they where generated by independent and identically-distributed samples. This can be useful in order to quantify Bell-inequality violations without the i.i.d. assumption.

Our approach to QKD goes beyond the philosophy of [1] in which there is still quantum mechanics, in particular, the validity of Tsirelson's bound [19] is assumed. In contrast, our approach is conceptually simpler in that *all* we assume is no-signaling. It is remarkable that, although our security is based on weaker assumptions, the secret key rates that we obtain are comparable to the ones where the adversary's attack is constrained by no-signaling plus quantum mechanics [6]. In particular, we obtain the optimal rate of one secret bit per singlet consumed. Our results also contribute to the understanding of quantum cryptography where the honest users do not have a complete control of their quantum apparatuses, or distrust them [9, 20].

QKD is a present-day technology. Entanglement-based protocols are usually implemented with a source that sequentially sends entangled pairs of systems to Alice and Bob. Each pair is measured in Alice and Bob's locations with the same two apparatuses. Those measuring apparatuses could generate outcomes depending on previous inputs. If this is the case, our assumptions for the security proof do not hold, because there is signaling between measuring events within the same lab. It would be desirable to have a security proof which accommodates this situation. Therefore, an important open problem is to obtain a security proof from weaker no-signaling assumptions.

VIII. ACKNOWLEDGEMENTS

LlM is supported by Caixa Manresa, the spanish MEC projects (FIS2008-00784 "TOQATA", FIS2007-60182, Consolider Ingenio 2010 "QOIT"), and the EU-IP programme "SCALA". RR is supported by the Swiss National Science Foundation, grant No. 200021-119868. MC is supported by the Excellence Network of Bavaria (TMP, QCCC) and the DFG grants CH 843/1-1 and CH 843/2-1. AW is supported by the U.K. EPSRC through the "QIP IRC" and an Advanced Fellowship, by a Royal Society Wolfson Merit Award, a Philip Leverhulme Prize, by the European Commission through IP "QAP", and by the Singapore Ministry of Education. JB is supported by an EPSRC Career Acceleration Fellowship.

[1] A. Ekert; Phys. Rev. Lett. **67**, 661 (1991).
[2] A. Einstein, B. Podolsky, N. Rosen; Phys. Rev. **47**, 777 (1935).
[3] J. S. Bell; Physics **1**(3), 195 (1964).
[4] J. F. Clauser, M. A. Horne, A. Shimony, R. A. Holt; Phys. Rev. Lett. **23**, 880 (1969).
[5] S. Braunstein, C. Caves; Ann. Phys. **202**, p. 22 (1990).
[6] R. Renner; *Security of Quantum Key Distribution*, PhD thesis, quant-ph/0512258.
[7] M. Koashi, A. Winter; Phys. Rev. A **69**, 022309 (2004).
[8] U. Leonhardt; Phys. Rev. Lett. **74**, 4101 (1995).
[9] A. Acín, N. Gisin, Ll. Masanes; Phys. Rev. Lett. **97**, 120405 (2006).
[10] Ll. Masanes, A. Acín, N. Gisin; Phys. Rev. A **73**, 012112 (2006).
[11] J. Barrett, L. Hardy, A. Kent; Phys. Rev. Lett. **95**, 010503 (2005).
[12] A. Acín, S. Massar, S. Pironio; New J. Phys. **8**, 126 (2006).
[13] R. Renner, R. Koenig; Proc. of TCC 2005, LNCS, Springer, vol. 3378 (2005).
[14] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, J. Oppenheim; Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005, J.Kilian (ed.) Springer Verlag 2005, vol. 3378 of Lecture Notes in Computer Science, pp. 386-406.
[15] Ll. Masanes; Phys. Rev. Lett. **102**, 140501 (2009).
[16] M. Christandl, R. Koenig, R. Renner; Phys. Rev. Lett. **102**, 020504 (2009).
[17] R. Koenig, R. Renner, C. Schaffner; IEEE Trans. Inf. Th., vol. 55, no. 9 (2009).
[18] J. L. Carter, M. N. Wegman; Journal of Computer and System Sciences, 18:143-154, 1979. M. N. Wegman, J. L. Carter; Journal of Computer and System Sciences, 22:265279, 1981.
[19] B. S. Tsirelson; Hadronic J. Suppl. **8**, 329 (1993).
[20] D. Mayers, A. Yao; quant-ph/9809039.